ECS Configuration Change Request

1. Originator	2. Log Date:	3. CCR #:	4. Rev:	5. Tel:	6. Rm #:	7. Dept.
Henry Baez	8 AUG 00	00-0806	—	301-925-1025	2101D	SED

8. CCR Title: Baseline Engineering Technical Directive for Solaris systems, sadmin and KCMS services.

9. Originator Signature/Date	10. Class	11. Type:	12. Need Date: 8/09/2000
Henry Baez 8/4/2000	II	CCR	

13. Office Manager Signature/Date	14. Category of Change:	15. Priority: (If "Emergency" fill in Block 28).
Randy Haynes 8/4/2000	Initial ECS Baseline Doc.	Routine

16. Documentation/Drawings Impacted:	17. Schedule Impact:	18. CI(s) Affected:

19. Release Affected by this Change:	20. Date due to Customer:	21. Estimated Cost:
5A		None - Under 100K

22. Source Reference: ☐NCR (attach) ☐Action Item ☐Tech Ref. ☐GSFC ☐Other:

23. Problem: (use additional Sheets if necessary)
Two vulnerabilities have been found in SunOS 5.7, 5.6, 5.5.1, and 5.5. The sadmin program has a buffer overflow vulnerability that may be exploited by a remote attacker to execute arbitrary instructions and gain root access. The Kodak Color Management System (KCMS) program vulnerability allows a malicious hacker to execute code that spawns a root shell for non-privilege users to get root access.

24. Proposed Solution: (use additional sheets if necessary)
Both the sadmind and KCMS program are not used in ECS custom code. Both services has been turn off in functionality lab testing without breaking anything. On each SunOS server disable the KCMS service and sadmind program in the /etc/inetd.conf file as per Engineering Technical Directive.

25. Alternate Solution: (use additional sheets if necessary)
Do nothing and risk that someone will use these exploites to damage or destory ECS data and systems.

26. Consequences if Change(s) are not approved: (use additional sheets if necessary)
If these changes are not implemented the systems may be exploited by a remote attacker to execute arbitrary instructions and gain root access.

27. Justification for Emergency (If Block 15 is "Emergency"):

28. Site(s) Affected: ☐EDF ☒PVC ☒VATC ☒EDC ☒GSFC ☒LaRC ☒NSIDC ☒SMC ☐AK ☐JPL ☐EOC ☐IDG Test Cell ☐Other

29. Board Comments:	30. Work Assigned To:	31. CCR Closed Date:

32. EDF/SCDV CCB Chair (Sign/Date): Byron V Peters 8/9/00	Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB
33. M&O CCB Chair (Sign/Date): W Bamford 15 Aug 00	Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
34. ECS CCB Chair (Sign/Date):	Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB

ORIGINAL